

### **REMARKS**

The office action dated April 7, 2006 has been received and carefully noted. The above amendments to the claims and the following remarks are submitted as a full and complete response thereto.

In accordance with the foregoing, claims 2, 3, 5-7, 10, 11-13, 14, 16, 21-23, 25-27, 29-31, 34-38, 40, 45, 46, and 47 and cancel claims 1, 15, 24, and 39, without prejudice or disclaimer. No new matter is being presented, and approval and entry are respectfully requested. As will be discussed below, it is also requested that all of claims 2-14, 16-23, 25-38, and 40-47 be found allowable as reciting patentable subject matter.

Claims 2-14, 16-23, 25-38, and 40-47 are pending and under consideration.

### **AMENDMENTS TO THE SPECIFICATION:**

The Specification is amended herein to resolve the minor informality described on page 2 of the office action, taking the Examiner's comments into consideration and directed to overcoming the objections thereto. The Applicants respectfully request that the Examiner withdraw the objections thereto.

### **REJECTION UNDER 35 U.S.C. § 103:**

*In the office action, at page 2, claims 1, 2, 5-15, 21-26, 29-39, and 45-47 were rejected under 35 U.S.C. § 103 as being unpatentable over McCann et al. (EP 1191763)*

*("McCann") in view of Williamson (EP 1107089) ("Williamson"). The office action took the position that McCann and Williamson disclose all the aspects of independent claims 1 and 24 and related dependent claims 2, 5-15, 21, 22, 23-26, 29-39, and 45-47. It is respectfully asserted that, for at least the reasons provided herein below, McCann and Williamson fail to teach or suggest the recitations of the pending claims. Reconsideration is requested.*

Independent claim 13 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, and if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login.

Independent claim 14, upon which claims 2-12 and 21 are dependent, recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting

identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, and if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a confirmation identifier from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal together with the password, the password being only used if the received confirmation identifiers are the same.

Independent claim 22 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a user ID to the subscriber terminal corresponding to the

mobile subscriber identification data and using the transmitted user ID in connection with login.

Independent claim 23 recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The method further includes transmitting a user ID to the data transfer device over a data transfer connection and using the transmitted user ID in connection with login.

Independent claim 37 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server

is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a second password from the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to also use the second password in connection with login.

Independent claim 38, upon which claims 25-36 and 45 are dependent, recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a

valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a confirmation identifier via the service access point to the data transfer device over the first data transfer connection and to transmit the same confirmation identifier to the subscriber terminal together with the password.

Independent claim 46 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is

configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a user ID to the subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system and the data transfer device is configured to use the user ID transmitted to the subscriber terminal in connection with login to the service access point.

Independent claim 47 recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit

the user ID via the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user ID transmitted to the data transfer device in connection with login to the service access point.

As will be discussed below, McCann and Williamson fail to disclose or suggest the elements of any of the presently pending claims.

McCann generally describes an authentication system in which a user requesting visiting access to the W-LAN is required to have a valid cellular mobile account, a portable computing device with a browser and a valid W-LAN card from another operator that administers a home authentication, authorization, and accounting (HAAA) server. The user inputs identity information that enables the HAAA to issue a personal identification number (PIN) which is encoded and forwarded to the user's mobile telephone. The encoded PIN is transferred to the browser to authenticate the requested visiting access to the W-LAN.

Williamson, in turn, generally describes an authentication process, which includes establishing a connection from a terminal device to a remote network/internet site, entering a user password and communicating the user password from the terminal device to the remote site, generating at the remote site an authentication security code, and establishing a second connection from the remote site to the user, transmitting a security code to the user through the second connection. In the process, the security code is entered at the terminal device and transmitted to the remote site through the first



connection. The security code entered at the terminal device is compared with the security code previously generated by the remote site, and if they match, the authentication is provided.

However, McCann and Williamson fail to teach or suggest, “if a valid access right exists, generating a **password**, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the **subscriber terminal**, and transmitting a **second password** from the service access point to the data transfer device over a data transfer connection, the second password **being also used** in connection with login,” as recited in independent claim 13. McCann is devoid of any teaching or suggestion of a transmission of two passwords. Similarly, although Williamson describes that in a login, a username and/or password may be used (paragraph [0014]), and subsequently a security PIN number generated by a remote server/host may be sent to the telecommunications device (paragraph [0015] and claim 1 of Williams), Williamson fails to teach or suggest, as in the present invention, that two passwords are transmitted to the user. That is, a password to the subscriber terminal and a second password to the data transfer connection. A combination of McCann and Williamson would fail to teach or suggest all the recitations of independent claim 13. For similar reasons, McCann and Williamson would fail to teach or suggest all the recitations of independent claim 37.

Referring to independent claim 14, McCann is devoid of any teaching or suggestion of a transmission of a password and a confirmation identifier. Similarly, although Williamson describes a security PIN number being generated as a password, Williamson does not teach or suggest, “transmitting a **confirmation identifier** from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal **together with the password**, the password **being only used** if the received confirmation identifiers are the same,” as recited in independent claim 14. The security PIN number of Williamson is not used together with a confirmation identifier to perform the process being recited in independent claim 14. A combination of McCann and Williamson would fail to teach or suggest all the recitations of independent claim 14 and related dependent claims. For similar reasons, McCann and Williamson would fail to teach or suggest all the recitations of independent claim 38 and related dependent claims.

Regarding independent claim 22, McCann and Williamson fail to teach or suggest, “if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal; and transmitting a user ID to the subscriber terminal corresponding to the mobile subscriber identification data and using the transmitted user ID in connection with login,” as recited in independent claim 22. In paragraphs [0013], [0014], and [0026] of McCann there is not teaching or suggestion

providing that a user ID is transmitted to the subscriber terminal as in the present invention. Instead, McCann discloses in those paragraphs that a PIN encoded with a registration number is transmitted to a handset of a mobile user. The registration number is public, and cannot be considered as a user ID that is user specific (See paragraphs [0022] and [0023] of McCann). A combination of McCann and Williamson would fail to teach or suggest all the recitations of independent claim 22. For similar reasons, McCann and Williamson would fail to teach or suggest all the recitations of independent claim 46.

Referring to independent claim 23, McCann and Williamson fail to teach or suggest all the recitations of independent claim 23. Williamson does not describe in paragraphs [0016] that a user ID is transmitted to the data transfer device. Specifically, similarly to McCann, Williamson fails to teach or suggest, “transmitting a user ID to the data transfer device over a data transfer connection and using the transmitted user ID in connection with login,” as recited in independent claim 23. Instead, Williamson describes that a security PIN is transmitted to the telecommunications device. The security PIN “provides the user’s identity,” shows that a user name is provided earlier in Williamson (See paragraph [0014] of Williamson). Thus, a combination of McCann and Williamson would fail to teach or suggest all the recitations of independent claim 23. For similar reasons, McCann and Williamson would fail to teach or suggest all the recitations of independent claim 47.

Accordingly, in view of the foregoing, it is respectfully requested that independent claims 13, 14, 22, 23, 37, 38, 46, and 47 and related dependent claims be allowed.

*In the office action, at page 14, claims 3, 4, 20, 27, 28, and 40 were rejected under 35 U.S.C. § 103 as being unpatentable over McCann et al. (EP 1191763) ("McCann") in view of Williamson (EP 1107089) ("Williamson") and further in view of Lantto et al. (U.S. Patent No. 5,537,457) ("Lantto"). The office action took the position that McCann, Williamson, and Lantto disclose all the aspects of claims 3, 4, 20, 27, 28, and 40. It is respectfully asserted that, for at least the reasons provided herein below, McCann, Williamson, and Lantto fail to teach or suggest the recitations of the pending claims. Reconsideration is requested.*

Independent claim 16, upon which claims 17-20 are dependent, recites a method for authenticating a user of a data transfer device, including setting up a data transfer connection from the data transfer device to a service access point, inputting identification data of a subscriber of a mobile communications system to the service access point, checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The data transfer connection between the data transfer device and the service access point is set up when the subscriber terminal is roaming. The method further includes informing the subscriber terminal that if the roaming by the subscriber

terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual, and implementing the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met.

Independent claim 40, upon which claims 41-44 are dependent, recites a system configured to authenticate a user of a data transfer device, including a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, and an authentication server linked to the service access point over a second data transfer connection. The service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection. The authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system. The data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, the first data transfer connection is set up when the subscriber terminal is roaming, and

the visited mobile communications system is configured to inform the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual, and the authentication server is configured to implement the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met.

As will be discussed below, McCann, Williamson, and Lantto fail to disclose or suggest the elements of any of the presently pending claims.

Dependent claims 3 and 4 depend from independent claim 14 and dependent claims 27 and 28 depend from independent claim 38. Because the combination of McCann and Williamson must teach, individually or combined, all the recitations of the base claim and any intervening claims of dependent claims 3, 4, 27, and 28, the arguments presented above supporting the patentability of independent claims 14 and 38 over McCann and Williamson are incorporated herein.

Lantto generally describes a method for handling calls in a mobile telephone system. The call is handled by an ISUP/IAM message which has a static relationship between the address of the visitor location register in the network in which the terminal roams, and the unique terminal identity.

However, Lantto does not cure the deficiencies of McCann and Williamson. Lantto is devoid of any teaching or suggestion of providing a confirmation identifier.

Similarly to McCann and Williamson, Lantto is silent as to teaching or suggesting, “transmitting a confirmation identifier from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal together with the password, the password being only used if the received confirmation identifiers are the same,” as recited in independent claim 14. Instead, Lantto limits its description to describing that if the visitor location register has no data record relating to the unique identity, an attempt is made to collect from the home location register of the called subscriber the data that is required to complete the connection, this data being stored in the visitor location register. If the attempt is successful and the called subscriber is active, the connection is set up in a known manner with the aid of this data. However, a combination of McCann, Williamson, and Lantto would fail to teach or suggest that a confirmation identifier is transmitted from a service access point to a data transfer device and transmitting the confirmation identifier to the subscriber terminal together with the password. Thus, a combination of McCann, Williamson, and Lantto would fail to teach or suggest all the recitations of independent claim 14 and related dependent claims. For similar reasons, McCann and Williamson would fail to teach or suggest all the recitations of independent claim 38 and related dependent claims.

Furthermore, dependent claim 20 depends from independent claim 16. The combination of McCann, Williamson, and Lantto must teach all the recitations of independent claim 16. On pages 18-19 of the office action, it is correctly recognized that

McCann, Williamson, and Lantto fail to teach or suggest, “informing the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual; and implementing the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met,” as recited in independent claim 16 and “the visited mobile communications system is configured to inform the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual, and the authentication server is configured to implement the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met,” as recited in independent claim 40. However, without providing any evidentiary support, the office action arrives to the presently claimed invention by taking Official Notice.

If the U.S. Patent and Trademark Office wishes to take Official Notice that the proposed structural and functional modification is notoriously well known, Applicants respectfully request to the Examiner that supporting evidence be provided. The Federal Circuit has cautioned that an Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed



invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998).

While "Official Notice" may be relied upon, as noted in MPEP §2144.03, these circumstances should be rare when an application is under final rejection or action under 37 CFR §1.113. Official Notice unsupported by documentary evidence should be only be taken by the Examiner where the facts asserted to be well known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known and only when such facts are of notorious character and serve only to "fill in the gaps" which might exist in the evidentiary showing made by the Examiner to support a particular ground of rejection. Further, the Applicants should be presented with the explicit basis on which the Examiner regards the matter as subject to Official Notice sufficient to allow the applicant a proper opportunity to challenge that assertion.

No such showing has been made in the present office action. It is submitted that the reason why no such showing was made is because McCann, Williamson, and Lantto fail to teach, suggest, or otherwise provide the motivation needed to make such a modification. "To support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination. It is to be noted that simplicity and hindsight are not proper criteria for resolving the issue of obviousness." *Ex Parte Clapp*, 227 USPQ 972, 973 (B.P.A.I. 1985).

Accordingly, in view of the foregoing, it is respectfully requested that independent claims 14, 16, 38, and 40 and related dependent claims be allowed.

**CONCLUSION:**

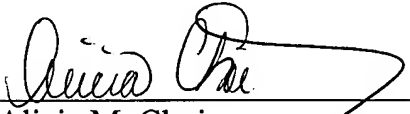
In view of the above, Applicant respectfully submits that the claimed invention recites subject matter which is neither disclosed nor suggested in the cited prior art. Applicant further submits that the subject matter is more than sufficient to render the claimed invention unobvious to a person of skill in the art. Applicant therefore respectfully requests that each of claims 2-14, 16-23, 25-38, and 40-47 be found allowable and this application pass to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time.

Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

  
Alicia M. Choi  
Registration No. 46,621

**Customer No. 32294**  
SQUIRE, SANDERS & DEMPSEY LLP  
14<sup>TH</sup> Floor  
8000 Towers Crescent Drive  
Tysons Corner, Virginia 22182-2700  
Telephone: 703-720-7800  
Fax: 703-720-7802

AMC;jkm

Enclosures: Additional Claim Fee Transmittal  
Check No. 14706